CLAIMS

What is claimed is:

1. A system to provide application-to-application enterprise security, the system comprising:

a security application program interface coupled to a client application operable on a first operating system to provide a security credential;

an authentication authority operable to receive the security credential from the security application program interface, the authentication authority further operable to generate a token and communicate the token to the security application program interface where the security credential is valid;

a store maintaining data operable to validate the security credential, the store in communication with the authentication authority to validate the security credential;

an application program interface coupled to the client application, the application program interface operable to communicate regarding the token; and

a server application operable on a second operating system to receive the token from the application program interface, the server application operable to communicate with the authentication authority to validate the token to enable the client application to use services of the server application.

2. The system of Claim 1, wherein the server application further comprises:

an application program interface to communicate with the application program interface of the client application; and

a security application program interface to communicate with the authentication authority.

3. The system of Claim 1, wherein the server application is operable to cache the token after validating the token with the authentication authority such that when the client application requests service of the server application, via the application program interfaces of the client application, the server application uses the cached token to validate the client application.

4. The system of Claim 1, wherein the token generated by the authentication authority comprises a string including at least a portion of the security credential.

5. The system of Claim 4, wherein at least a portion of the token is in Extensible Markup Language format.

6. The system of Claim 4, wherein at least a portion of the token is in Security Assertion Markup Language format.

7. The system of Claim 4, wherein the token includes information related to an expiration date of the token.

8. The system of Claim 1, wherein validating the token by the authentication authority includes determining whether the authentication authority created the token.

9. A method for providing application-to-application enterprise security, the method comprising:

communicating a security credential from a client application operable on a first operating system to an authentication authority;

communicating information related to the security credential between the authentication authority and a data store to determine whether the security credential is valid;

generating a token by the authentication authority when the security credential is valid;

communicating the token to the client application;

providing, by the client application, the token to a server application, the server application operable on a second operating system; and

validating, by the server application, the token before providing access to services of the server application by the client application.

10. The method of Claim 9, wherein the server application is provided with a security application program interface coupled to the server application operable for validating the token with the authentication authority.

11. The method of Claim 9, wherein the client application is provided with an application program interface coupled to the client application operable for communicating the token to an application program interface of the server application.

12. The method of Claim 9, wherein validating the token by the server application further comprises:

communicating information related to the token to the authentication authority;

determining, by the authentication authority, whether the token is authentic; and

receiving validation related information from the authentication authority.

13. The method of Claim 12, wherein the information related to the token is the token.

14. The method of Claim 12, wherein the information related to the token is a portion of data comprising the token.

15. The method of Claim 12, wherein the authentication authority determines whether the authentication authority generated the token to validate the token.

16. The method of Claim 15, wherein the authentication authority determines whether the token has expired.

17. The method of Claim 12, wherein the authentication authority determines whether the token has expired.

18. The method of Claim 9, wherein the token includes a portion of the security credential in a string format.

19. The method of Claim 18, wherein the token includes at least an information related to an expiration date of the token.

20. The method of Claim 18, wherein the token is encrypted.

21. The method of Claim 18, wherein the string format of the token is further defined as an Extensible Markup Language format.

22. The method of Claim 18, wherein the string format of the token is further defined as Security Assertion Markup Language format.

23. The method of Claim 9, wherein the client further includes an application program interface coupled to the client application for communicating with the server application and wherein the client application further includes a security application program interface coupled to the client application to communicate with the authentication authority.

24. The method of Claim 9, wherein the security credential is further defined as including a password and user identification.

25. The method of Claim 24, wherein the security credential is further defined as encrypted and the data store is further defined as a data store maintaining user identifications and passwords.

26. The method of Claim 9, wherein the security credential is an X.509 certificate and the data store is a certificate authority.

27. The method of Claim 26, further comprising:

communicating the X.509 certificate from the authentication authority to the certificate authority;

validating the X.509 certificate by the certificate authority; and

communicating validation information to the authentication authority.

28. A system to provide application-to-application enterprise security, the system comprising:

a first security application program interface coupled to a first application to provide a first security credential;

a second security application program interface coupled to a second application to provide a second security credential;

an authentication authority operable to receive the first and second security credentials from the first and second security application program interfaces, the authentication authority further operable to generate tokens and communicate the tokens to the first and second security application program interfaces where the first and second security credentials are valid;

a store maintaining data operable to validate the first and second security credentials, the store in communication with the authentication authority to validate the first and second security credentials;

a first application program interface coupled to the first client application, the first application program interface operable to communicate regarding tokens; and

a second application program interface coupled to the second client application and operable to receive the token from the first application program interface, the second security application program interface operable to communicate with the authentication authority to validate the token to enable the first application to use services of the second application and wherein the first second application program is operable to receive the token from the second application program interface, the first security application program interface operable to communicate with the

authentication authority to validate the token to enable the second application to use services of the first application.

29. The system of Claim 28, wherein the tokens generated by the authentication authority are further defined as a first token generated by the authentication authority for the first application based on the first security credential and a second token generated by the authentication authority for the second application based on the second security credential.

30. The system of Claim 29, wherein the first and second tokens are further defined as data provided in a string format including at least portions of the first and second security credentials, respectively.

31. The system of Claim 30, wherein the first the second tokens include an expiration date.

32. The system of Claim 30, wherein the string format of the first and second tokens is further defined as Extensible Markup Language Format.

33. The system of Claim 30, wherein the string format of the first and second tokens is further defined as Security Assertion Markup Language Format.